
CYBER *Practicals*

Virtual Machine

Release 1.0

Howard Chivers

Feb 21, 2017

CONTENTS

1	Getting Started	2
1.1	The Virtual Machine	2
1.2	Exercise Documentation	2
1.3	Accessing the Machine	3
2	Student Interface	4
2.1	Usermin	4
2.2	Web Shell	5
3	Installing an Exercise	7
4	VM Administration	9
4.1	Standard Interfaces	9
4.2	Admin Accounts	10
4.3	Database Accounts	10
4.4	Distribution Packaging	10
4.5	Answer Sheets	11
4.6	Deployment	11

The Cyber-Practicals Virtual Machine is the host for practical exercises in cyber security; it hosts the experiment together with work and answer sheets.

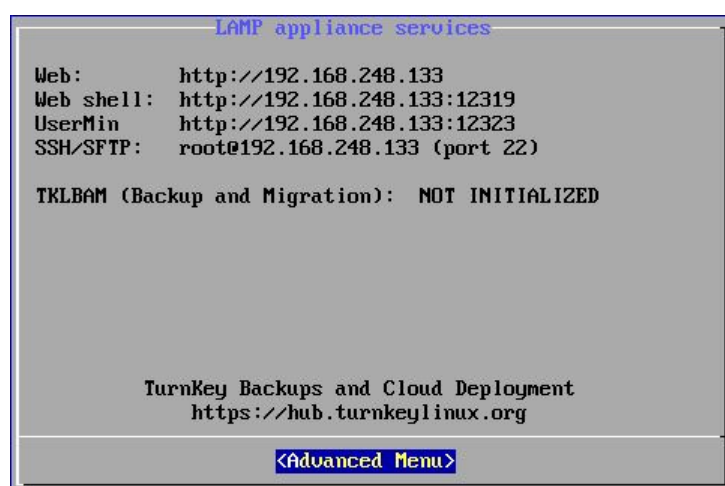
The VM is based on the Turnkey LAMP and does not host a desktop; the normal student interface is via browser access to Usermin for file management and editing, and a Web-Shell to run programs.

The first sections of this guide provide information for students using pre-configured machines, the next describes how to build an exercise from the distribution package and the base vm, finally further VM information is provided for administrators.

GETTING STARTED

1.1 The Virtual Machine

When the Virtual Machine is started it will boot Debian Linux and display the standard Turnkey control panel:



```
LAMP appliance services
Web:      http://192.168.248.133
Web shell: http://192.168.248.133:12319
UserMin   http://192.168.248.133:12323
SSH/SFTP: root@192.168.248.133 (port 22)

TKLBAM (Backup and Migration): NOT INITIALIZED

TurnKey Backups and Cloud Deployment
https://hub.turnkeylinux.org

<Advanced Menu>
```

This is a keyboard-only interface; the 'Advanced' menu will allow you to shutdown the machine and configure the IP address, either by requesting a new address via DHCP or by providing a fixed IP address. Normally all you need to do is to note the IP address that has been assigned.

Because this interface does not use a mouse, you will need to click somewhere on the screen to move the keyboard focus to the interface, and use an escape sequence to return to the host (in vmware ctrl-alt).

This screen should now be minimised, since it is not used during the experiments.

Note: At the end of your session use the advanced menu to close the server, otherwise you may lose some of your work.

1.2 Exercise Documentation

Open a web browser and navigate to <http://<vm-ip-address>> (the IP address you noted above).

The front page will provide links to exercise worksheets and other related information. It will also provide links to Usermin and the Webshell, described in the next section.



1.3 Accessing the Machine

Two applications are used to run experiments, both of which are accessed via a browser. The Web Shell (shellinabox) provides a command-line interface to the Linux bash shell and is used to run programs, Usermin provides access to a number of management modules, including a file manager which includes an editor and upload/download facilities.

These applications are linked from the webserver front page, and may also be accessed directly by specifying the port as part of the IP address:

Web Shell <vm ip address>:12319

Usermin <vm ip address>:12323

SSH <username>@<vmip address> (port 22)

Unless your instructor has given you other information, the student account is:

User student

Password golyeeHug6

Known Browser Issues

The Microsoft Edge browser will not access localhost addresses, if you are running the VM locally this browser cannot be used.

The Web Shell (shellinabox) may not display correctly on some versions of Microsoft Internet Explorer, this can be resolved by selecting compatibility mode for the problem page.

STUDENT INTERFACE

In addition to the webserver, users have access to a Web Shell and the Usermin control panel. Usermin allows the user to run command-line instructions; however, the Web Shell is usually used to run programs, and must be used to run interactive programs.

The Usermin control panel provides a file manager, which includes upload and download capability and a text editor which can be used for text and software. This lightweight distribution does not provide a desktop and therefore requires some familiarity with the linux shell; however, the Usermin interface simplifies file management for non-expert users.

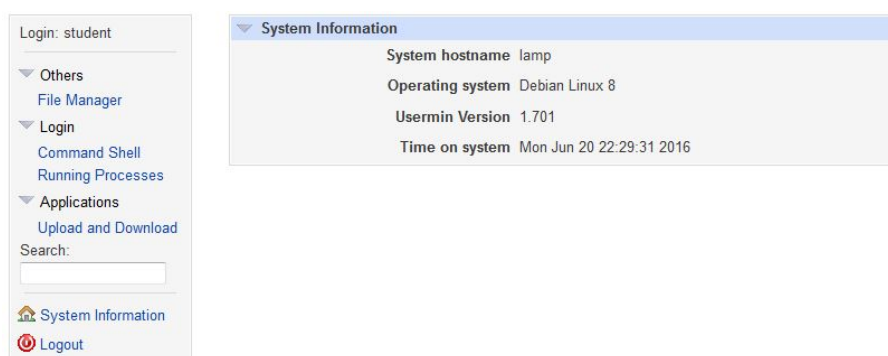
Unless your instructor has given you other information, the student account is:

User student

Password golyeeHug6

2.1 Usermin

The module is accessed using a browser via the control panel or directly via port 12323, see *Getting Started*. After login the following page is displayed:






The control panel on the left lists modules available to students; the most useful of these is the file manager which can also be used for uploading and downloading single files. (The upload and download module provides more extensive functions which include uploading and unpacking compressed archives.)

Module Index Module configuration

Filemin

/home/student/dev/ 🔍 + 📄 ⬇️ ☰ ☰ ☰ ✂️ 📄 📄 📄 ⚙️ 👤 ✖️ 🏠 🌐

Pages: 1
Total: 1 files and 0 folders

Name	Actions	Size	Owner User	Permissions	Last Modification Time
 pwcheck.py	 	1.02 kB	student:users	0644	2016/06/20 - 15:06:14

The File Manager module displays a set of iconised actions above a file listing. (Hover the mouse over an icon for tooltips if the icons seem obscure). Files that may be edited have a pencil icon in the actions section.

The manager will open at the /home/ folder, under which is the students' file system: /home/student.

The editor will open in an edit box that resizes as you add lines, and is code-sensitive:

```

/home/student/dev/print3.py
1 # short python program
2
3 for i in range(3):
4     print('{:d}: Hullo Again'.format(i))
5
Save Save and close

```

[← Return to previous page](#)

2.2 Web Shell

The web shell is accessed using a browser at port 12319, see *Getting Started*. The interface is similar to a standard command-line terminal; the shell is *bash* which supports up-down arrow to select previous commands.

```

lamp login: student
Password:
Last login: Sun Jul 10 10:01:31 UTC 2016 from 127.0.0.1 on pts/0
Linux lamp 3.16.0-4-amd64 #1 SMP Debian 3.16.7-ckt25-2 (2016-04-08) x86_64
Welcome to Lamp, TurnKey GNU/Linux 14.1 / Debian 8.5 Jessie

System information (as of Sun Jul 10 12:55:08 2016)

System load: 0.76          Memory usage: 32%
Processes:   97           Swap usage:   0%
Usage of /:  8.3% of 16.61GB IP address for eth0: 192.168.132.128

student@lamp ~$

```

A right-click in the window can be used to copy/cut/paste in addition to setting display properties such as the use of colour.

Most exercises that require programs to be run will execute from the command line. For example:

```
student@lamp ~/dev$ python3 print3.py
0: Hullo Again
1: Hullo Again
2: Hullo Again
student@lamp ~/dev$
```


INSTALLING AN EXERCISE

Cyber-practicals exercises may be downloaded as pre-built virtual machines, or installed on the base VM from a source distribution package. This section describes how to install the distribution package, the process is automated and results in a considerable saving in storage and download bandwidth.

Usually, students will not need to build an exercise from its distribution, unless they have downloaded exercises for their own study; if in doubt ask your instructor.

The base virtual machine is distributed as an Open Virtualization Format (OVF) file; such files can be loaded and run in many popular virtual environments (e.g. VMWare, VirtualBox). After building the machine, run it as described in the previous sections; since the base machine does not have an installed exercise there will not be any pre-built documentation.

Note: Only one exercise can be installed in a VM at a time and the install process requires the VM to be in its base state. If you wish to recycle a VM then snapshot the base configuration before install.

The standard exercises are intended to be deployed to users desktops, or behind a managed interface to a virtual infrastructure; they must not be deployed to a public cloud. See the *VM Administration*.

Before installation:

- The distribution package is a compressed (.zip) file. Briefly review the `INSTALL_README` file within the zip to check if there are any special instructions; very few exercises have special requirements.
- It may be necessary to access to the Internet to download standard software packages. Modify the default (host only) network setting of the VM to allow network access during the installation.

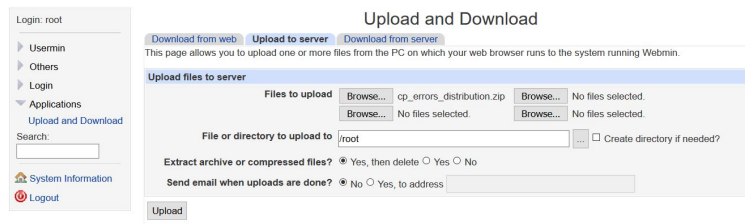
To install an exercise on the base VM:

- Log into Usermin (port 12323) as root.

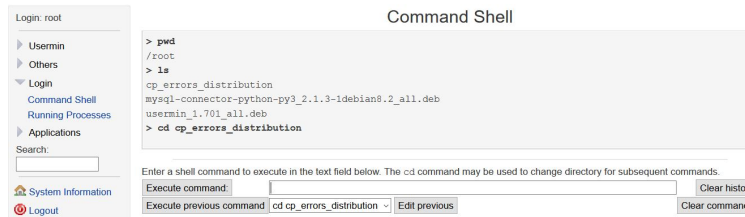
User root

Password TerHoojEpy

- Upload and decompress the distribution package to the `/root` directory. The upload manager from Usermin is able to upload and decompress at the same time.



- Only a few commands are required to install, so they can be run from the Usermin command line. By default it should open at `/root` which contains a folder starting `cp_`. Move into that directory (for example, `cp_errors_distribution`).



- To install the exercise first make `install.sh` executable, and then execute it:

```
chmod 775 install.sh
./install.sh
```

The install script will build the documentation, place any data or programs required in the student home directory, and configure any software necessary for the exercise.

After the installer has run return the VM to host-only networking. At this stage, if required, the VM can be shut down and copied for use by several students. If you wish to modify the machine (e.g. remove answer sheets), see the [VM Administration](#) section.

Note: Exercises may not work from the root user, to use the exercise log out of the root account and log back in as student.

VM ADMINISTRATION

The following information is provided for institutional system administrators, it should not be needed by users.

4.1 Standard Interfaces

In addition to Usermin, Shellinabox and SSH, the VM supports Webmin. Webmin has modules for managing the system, including MySQL and Usermin. The MySQL database can also be managed via Adminer.

Cyber Practicals



These applications are linked from the https webserver front page shown above (you will have to accept a self-signed certificate) and may also be accessed directly by specifying the port as part of the IP address:

Web Shell <vm ip address>:12320

Webmin <vm ip address>:12321

Adminer <vm ip address>:12322

SSH <username>@<vmip address> (port 22)

In addition to the standard Turnkey VM configuration, the base VM also includes the user configurations (student, staff and database user), a separate webserver document root for exercises (see below) and additional installed software:

- Python3
- Pip (which is only enabled for Python3)
- build-essential python3-dev (to allow building from source)
- mysql.connector (python interface to the MySQL API)
- php-sqlite

4.2 Admin Accounts

There are two admin accounts, *root* and *staff*. The *staff* account is a restricted account which is able to modify the contents of the website. The document root of the website is at:

```
/home/staff/docroot/
```

Account details are:

Account	Password
root	TerHoojEpy
staff	RouWeadLog
student	golyeeHug6

4.3 Database Accounts

The MySQL database has two accounts, a root administration account and a user (*cyber-practicals*) which is the normal access for experiments. Some experiments use other databases (e.g. SQLite) which are installed with the experiment. The user account is unable to grant privileges but can carry out most database operations. The database accounts are:

Account	Password
root	Pr1agDidem
cyber-practicals	1kjg4G1iu5

4.4 Distribution Packaging

The standard packaging of *cyber-practicals* exercises is straightforward. The install script may be used to apt-get software packages or configure installed software, and also uses the following folders:

- `document_root`
- `student_root`
- `python_modules`

The install script replaces the default *index.htm* file in the document root `/home/staff/docroot/` with the contents of the `document_root` folder; the ownership is set to *staff*.

Similarly, the contents of the `student-root` folder is copied to `/home/student/` and the ownership set to *student*. Usually student files (e.g. Python programs) will be placed in a sub-folder `working`. Note that these ownerships may be assumed by installed software, which may lose access if *staff* or *student* files are subsequently modified by a user working as *root*. The exercises are built assuming that they will be conducted by a *student* user.

The `python_modules` folder contains an installation script `install_required.py` which installs modules listed in the `required_modules` file. This file may contain blank lines and comment lines that begin with `#` but is otherwise a line separated list of python module names that are installed in order.

The `python_modules` folder may also contain any special python source distributions required, which are installed if the corresponding module names are present in the `required_modules` file.

When python source distributions are installed, the script checks for two special package methods: `postinstall` and `test`. `postinstall` is expected to contain any further build scripts for the experiment, such as building and populating a database, and `test` is expected to provide installation unit testing. If these are both found `postinstall` will be run before `test`.

4.5 Answer Sheets

If you prefer to remove answer sheets from the VM after installation, log in as `staff` user and delete them from the `answer` directory in the webserver root, and also remove the corresponding pdf from the `papers` directory.

4.6 Deployment

The standard student interface to the VM uses `http` (not `https`) to simplify the use of the VM when deployed to a local host/desktop. Unencrypted access would also be acceptable if the VMs were depoloyed in a protected virtual infrasructure, usually behind a managed interface.

The standard Turnkey distribution uses self-signed certificates which would undesirably prompt students to set vulnerable browser security exceptions. This is the reason for the default unencrypted interface - any other requires knowledge of a particular Institutions' infrastructure, and suitable keys. Unmodified VMs should not, therefore, be deployed to the public cloud or to servers with unrestricted access.

If required the base VM can be modified by a UNIX administrator to use secure interfaces, it is necessary to:

- Load suitable keys to the VM.
- Modify Usermin to use 'SSL' (it will then select the installed secure protocol).
- Disable port 12319 (Students will need to use port 12320 for WebShell).